

HANDREIKING INFORMATIEBEVEILIGINGS- MAATREGELEN SOCIAAL DOMEIN

VISD is een programma van de VNG dat wordt uitgevoerd in samenwerking met KING

Opgesteld door	VNG/KING
Datum	3 oktober 2014
Versie	0.9

Colofon

Naam document

Handreiking informatiebeveiligingsmaatregelen sociaal domein

Versiebeheer

Het beheer van dit document berust bij het Programma Vervolg Informatievoorziening Sociaal Domein tot uiterlijk 31-12-2014.

Copyright

© 2014 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door KING;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Leeswijzer

Dit product maakt onderdeel uit van het programma VISD (informatievoorziening Sociale Domein) en helpt gemeenten om hun informatiehuishouding op tijd en veilig aan te passen aan de nieuwe taken.

Doel

Het doel van dit document is de veilige gegevensverwerking en -uitwisseling ook binnen de informatievoorziening in het sociale domein te waarborgen en om de additionele informatiebeveiligingsrisico's die door de decentralisatie ontstaan voor gemeenten en partners te verminderen. Deze additionele risico's zijn geanalyseerd en om deze te verminderen dienen passende maatregelen genomen te worden bij gemeenten, partners, op knooppunten, op koppelvlakken en bij en/of door leveranciers. De maatregelen zijn zowel technisch, procedureel, organisatorisch als beleidsmatig van aard (integraliteit) en dienen aan te sluiten bij het niveau van gevoeligheid en de kwetsbaarheid van de informatie.

Doelgroep

Dit document is van belang voor onder andere de informatiebeveiligingsfunctionarissen / Chief Information Security Officers (CISO) van gemeenten, de verantwoordelijke voor het inrichten van de nieuwe taken naar aanleiding van de decentralisaties binnen gemeenten en de betrokken architecten, proces- en informatiesysteemeigenaren bij de decentralisaties.

Inhoud

1	Managementsamenvatting	6
2	Inleiding	8
2.1	Informatiebeveiliging en de decentralisaties	8
2.2	Hoe te lezen	8
3	Aanpak uitgevoerde analyses	10
4	Resultaten uitgevoerde analyses	12
4.1	Meest relevante bedreigingen	12
4.2	Meest relevante maatregeldoelstellingen	13
4.3	Vervolgstappen	14
	Bijlage 1: maatregeldoelstellingen informatievoorziening sociaal domein	16

1 Managementsamenvatting

Gemeenten hebben te maken met een normenkader op het gebied van informatieveiligheid, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit normenkader kent een aanpak om vast te stellen of een nieuw proces en onderliggend informatiesysteem door de BIG voldoende beveiligd wordt. Deze aanpak bestaat uit een baselinetoets BIG eventueel gevolgd door een diepgaande risicoanalyse BIG en/of een Privacy Impact Assessment (PIA).

De invoering van de drie decentralisatie heeft een grote impact op de informatievoorziening van gemeenten. KING heeft om die reden een programma opgezet om gemeenten hierbij te ondersteunen. Het opstellen van een Programma van Eisen (PvE) is onderdeel hiervan. Vanuit de actielijn PvE is een baselinetoets BIG uitgevoerd bij een aantal Living Labs.

Na het uitvoeren van de baselinetoets BIG op de informatievoorziening in het sociaal domein is vastgesteld dat voor de informatiesystemen binnen het sociale domein het beschermingsniveau boven de BIG eisen liggen. Het gevolg hiervan was dat voor de informatievoorziening in het sociale domein, vanuit de actielijn PvE, een diepgaande risicoanalyse is uitgevoerd.

De conclusie van deze uitgevoerde diepgaande risicoanalyse is dat de meest belangrijke maatregeldoelstellingen, die bovenop de BIG eisen liggen en waarbij het noodzakelijk is om expliciet actie op te ondernemen, betrekking hebben op:

- Het niet goed of niet tijdig uitvoeren van beheeractiviteiten. Dit voorkomt men door het tijdig (in een zo vroeg mogelijk stadium) en duidelijk beschrijven, toewijzen en vastleggen van de verantwoordelijkheden, bevoegdheden, taken en werkafspraken van zowel de interne en externe ICT-dienstverlener(s) op het gebied van beheeractiviteiten. Het is ook noodzakelijk om gebruik te maken van patchmanagement, wijzigingsbeheer en ontwikkel- en testprocedures. Denk hierbij ook aan geheimhoudings- en bewerkersovereenkomsten.
- Het voorkomen dat de continuïteit van kritische bedrijfsprocessen en de hierbij betrokken informatievoorziening worden verstoord. Om de continuïteit niet te verstoren is het noodzakelijk om gebruik te maken van back-up en restore-procedures, redundant uitvoeren van kritische componenten.
- Het voorkomen van ongeautoriseerde toegang tot het informatiesysteem en de gegevens daarin. Dit betreft zowel de fysieke toegang door gebruikers en beheerders tot de computerruimte als de toegang op infrastructureel en systeem niveau. Denk hierbij ook aan het werken op afstand en met behulp van mobiele apparaten. Besteed expliciet aandacht aan toegang door externe partijen (leveranciers). Maar ook het veilig vernietigen van gegevens dient hier een onderdeel van uit te maken.
- Het voorkomen van onzorgvuldige (opzettelijk of onopzettelijk) omgang met de gegevens die in het informatiesysteem zijn opgeslagen, door gebruikers en beheerders. Dit dient zowel met technische middelen afgedwongen te worden als door middel van opleiding en communicatie (awareness) worden voorkomen.

Ook de score met betrekking tot persoonsgegevens en de verwerking hiervan ligt hoger dan het basisbeveiligingsniveau. Dit betekent dat ook aanvullend onderzoek noodzakelijk is om beter inzicht in de privacyrisico's te krijgen. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft hier het voortouw in genomen en voert de Privacy Impact

Assessments (PIA's) uit. De uitkomsten van deze PIA's zullen onder andere via het VISD-programma met alle gemeenten worden gedeeld.¹

¹ Zie voor extra achtergrondinformatie de beleidsvisie "Zorgvuldig en bewust: gegevensverwerking en privacy in een gedecentraliseerd sociaal domein" en de begeleidende brief van minister BZK (<https://zoek.officielebekendmakingen.nl/kst-32761-62>) en de informatie hierover op de visd.nl (<https://www.visd.nl/gegevensuitwisseling-en-privacy/nieuws/beleidsvisie-gegevensverwerking-en-privacy>)

2 Inleiding

Gemeenten staan voor een enorme uitdaging om op een integrale wijze invulling te geven aan het gehele sociaal domein van werk, zorg en jeugd.² Tegelijkertijd wordt van gemeenten gevraagd om een omvangrijke besparing te realiseren en in meer gevallen een beroep te doen op de zelfredzaamheid van haar burgers. Deze transformatie kan mede succesvol worden door een optimale informatievoorziening voor de stakeholders in het werkveld van het sociale domein. Voor de ontwikkeling van producten voor de Informatievoorziening Sociaal Domein wordt gebruik gemaakt van de ervaringen uit de Living Labs.³ De Living Labs zijn proeftuinen (experimentele omgevingen) waar vijf gemeenten samen met anderen oplossingen uitproberen en ontwikkelen op verschillende onderdelen van de Informatievoorziening Sociaal Domein. De ervaringen en inzichten van deze Living Labs zijn generiek gemaakt zodat deze voor andere gemeenten bruikbaar zijn.

2.1 Informatiebeveiliging en de decentralisaties

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. De drie decentralisaties voor werk, zorg en jeugd zijn niet als uitgangspunt genomen bij het opstellen van de BIG waardoor het, op basis van de uitgevoerde risicoanalyse, nodig is om voor de drie decentralisaties additionele specifieke maatregelen te treffen.⁴ Binnen de drie gedecentraliseerde domeinen wordt (zeer) privacygevoelige informatie van burgers verzameld, verwerkt en uitgewisseld. Er is gemeenten en partners dan ook veel aan gelegen om deze informatie goed te beveiligen.

2.2 Hoe te lezen

Afhankelijk van de informatiebeveiligingsrisico's en de door de gemeente gemaakte inrichtingskeuzes voor de drie decentralisaties, zijn mogelijk additionele specifieke maatregelen nodig ten opzichte van de BIG. Om gemeenten handvatten te bieden welke relevante documenten kunnen worden gebruikt om informatiebeveiliging vanaf het begin mee te nemen, wordt een koppeling gelegd met de aandachtspunten vanuit de decentralisaties. In dit document wordt een overzicht gegeven van (operationele) documenten die gemeenten helpen bij de implementatie van de beveiligingsmaatregelen. Uiteraard is hierbij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) het uitgangspunt.

Structuur

De indeling van dit document is als volgt:

Hoofdstuk 2, geeft een inleiding over informatiebeveiliging in relatie tot de decentralisaties.

Hoofdstuk 3, gaat kort in op de gehanteerde aanpak.

² <http://www.rijksoverheid.nl/onderwerpen/gemeenten/decentralisatie-van-overheidstaken-naar-gemeenten>

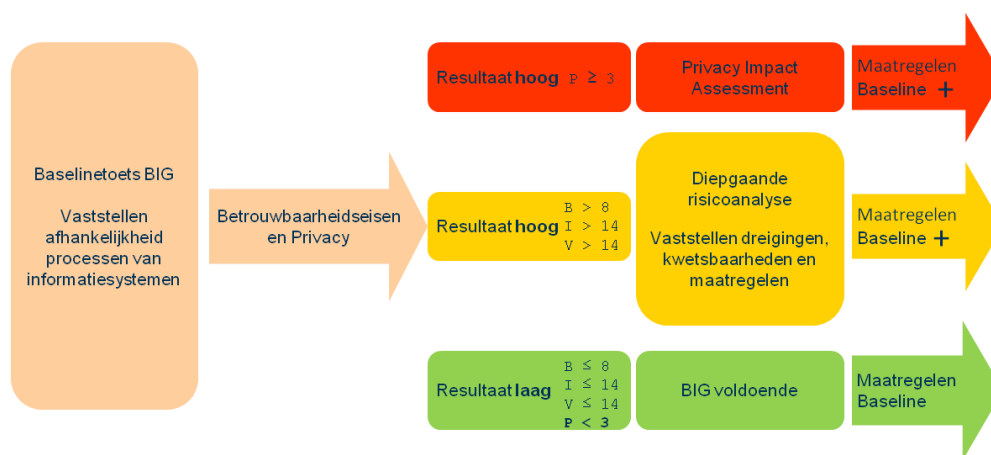
³ De Living Labs met betrekking tot de Informatievoorziening Sociaal Domein zijn Eindhoven, Enschede, Leeuwarden, Utrecht en Zaanstad (<https://www.visd.nl/visd/de-living-labs>).

⁴ Om vast te stellen dat het niveau van de BIG voldoende is, moet een baselinetoets BIG (<http://www.ibdgemeenten.nl/wp-content/uploads/2014/06/14-0609-BIG-Baselinetoets-v1.0.pdf>) uitgevoerd worden (zie hoofdstuk 3 'Aanpak uitgevoerde analyses').

Hoofdstuk 4, geeft een overzicht van de meest relevante bedreigingen, maatregeldoelstellingen en de te volgen vervolgstappen.

3 Aanpak uitgevoerde analyses

Voor belangrijke systeemwijzigingen of als een project wordt opgestart om te komen tot een nieuw informatiesysteem binnen de gemeente, dient een baselinetoets van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) te worden uitgevoerd. Wanneer hieruit volgt dat de systeemwijziging of het nieuwe informatiesysteem binnen de BIG valt, kan worden volstaan met het invoeren van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Wanneer de eisen boven een bepaalde grens uitstijgen, is het noodzakelijk om een diepgaande risicoanalyse en/of een Privacy Impact Assessment (PIA) uit te voeren. Zie figuur 1 voor de samenhang tussen de baselinetoets BIG, de diepgaande risicoanalyse en de PIA. Doelstelling van de diepgaande risicoanalyse is om in kaart te brengen welke maatregelen aanvullend op de BIG noodzakelijk zijn om het juiste niveau van beveiliging te realiseren.



Figuur 1 samenhang tussen de baselinetoets BIG, de diepgaande risicoanalyse en de PIA

In de baselinetoets BIG is het uitgangspunt dat het proces afhankelijk is van de informatievoorziening. In de diepgaande risicoanalyse ligt de nadruk op de informatievoorziening die het proces ondersteunt. Hierbij geldt dat hoe hoger het risico, des te meer c.q. zwaardere maatregelen worden aanbevolen. De maatregelen die worden aanbevolen omvatten het volledige scala van organisatie tot technologie.

De score op de betrouwbaarheidseisen beschikbaarheid, integriteit en vertrouwelijkheid (BIV in figuur 1) uit de baselinetoets BIG zijn bepalend of er een diepgaande risicoanalyse noodzakelijk is. De score op de eisen met betrekking tot persoonsgegevens (P in figuur 1) en de verwerking hiervan uit de baselinetoets BIG zijn bepalend of er een PIA noodzakelijk is.

De diepgaande risicoanalyse volgt een quick scan aanpak om ervoor te zorgen dat op een pragmatische en effectieve manier de juiste zaken in kaart worden gebracht. De diepgaande risicoanalyse bestaat uit drie hoofdstappen:

1. Het in kaart brengen van het Informatiesysteem: Dit betreft het in kaart brengen van de onderdelen van de informatievoorziening conform het MAPGOOD model. Dit is nodig om in de volgende stap de bedreigingen goed in kaart te kunnen brengen. MAPGOOD staat voor: Mens, Apparatuur, Programmatuur, gegevens, organisatie, Omgeving en Diensten.

2. Analyse van de dreigingen: Het in kaart brengen van de dreigingen die relevant zijn voor het te onderzoeken informatiesysteem, met per dreiging het potentiële effect en de kans op optreden.
3. Bepalen van de maatregelen: Formuleren van maatregelen op het niveau van doelstellingen, op basis van de eisen en relevante bedreigingen.

Een uitgebreidere beschrijving over de gehanteerde aanpak is te vinden op de IBD website (www.ibdgemeenten.nl) en dan specifiek in onderstaande documenten:

- [Baselinetoets BIG](#) (inclusief een [voorbeeld uitwerking](#))
- [Diepgaande risicoanalyse](#) (inclusief een [voorbeeld uitwerking](#))

4 Resultaten uitgevoerde analyses

In dit hoofdstuk worden de meest relevante bedreigingen en maatregeldoelstellingen beschreven die uit de uitgevoerde analyse met betrekking tot de informatievoorziening in het sociaal domein naar voren zijn gekomen. In bijlage 1 'maatregeldoelstellingen informatievoorziening sociaal domein', wordt het complete overzicht van de maatregeldoelstellingen uit de uitgevoerde analyse beschreven. Als laatste wordt een advies gegeven met betrekking tot de vervolgstappen.

4.1 Meest relevante bedreigingen

In deze paragraaf wordt een overzicht gegeven van de meest relevante bedreigingen die uit de uitgevoerde diepgaande risicoanalyse naar voren zijn gekomen, waardoor verlies aan beschikbaarheid, integriteit of vertrouwelijkheid van de informatievoorziening kan ontstaan. Hier dient expliciete aandacht aan te worden besteed. Deze meest relevante bedreigingen, zijn:⁵

- Incident: Nalatig menselijk handelen met betrekking tot programmatuur.
 - Ontwerp, programmeer, implementatie beheer/onderhoudsfouten.
 - Introductie van virus en dergelijke door gebruik van door de gemeente ongescreende/ongeautoriseerde programma's.
 - Gebruik van de verkeerde (verouderde) versie van de programmatuur.
 - Slechte documentatie. Bijvoorbeeld: gebruikersdocumentatie en/of beheerhandleidingen.

Bijvoorbeeld: Bij een webbased of SaaS oplossing kunnen (eind)gebruikers gebruik maken van een thuis PC of een eigen tablet.
- Incident: Onopzettelijk menselijk handelen met betrekking tot programmatuur.
 - Fouten door niet juist volgen van procedures.
 - Installatie van malware en virussen door gebruik van onjuiste autorisaties.

Bijvoorbeeld: Systeembeheerders en/of eindgebruikers hebben meer rechten op de gemeentelijke informatiesystemen dan noodzakelijk om hun werkzaamheden uit te kunnen voeren.
- Incident: Opzettelijk menselijk handelen met betrekking tot programmatuur.
 - Manipulatie voor of na ingebruikname.
 - (ongeautoriseerde) functieverandering en/of toevoeging.
 - Installatie van virussen, trojaanse paarden en dergelijke.
 - Kapen van autorisaties van collega's.
 - Illegaal kopiëren van programmatuur.
 - Oneigenlijk gebruik of privégebruik van bedrijfsprogrammatuur.

Bijvoorbeeld: De kans is aanwezig dat op de thuiswerkplek (of mobiele apparaat zoals een tablet) ongescreende/ongeautoriseerde software draait of op geïnstalleerd wordt. De kans is aanwezig dat autorisaties, gebruikersnamen en wachtwoorden, gedeeld worden met collega's. Vaak om te zorgen voor voortgang van het proces.

⁵ De dreigingen zijn in de vorm van incidenten verwoord en per incident is gekeken hoe groot de invloed ervan is op de werking van het informatiesysteem (de schade) en wat de kans is op het optreden van de betreffende dreiging.

- Incident: Via apparatuur met betrekking tot gegevens
 - Fysieke schrijf- of leesfouten.
 - Onvoldoende toegangsbeperking tot apparatuur.
 - Fouten in interne geheugens.
 - Aftappen van gegevens.

Bijvoorbeeld: Bij SaaS oplossingen staan de gegevens op apparatuur van derden, dit geldt ook als de gemeentelijke informatiesystemen op de infrastructuur van derden (uitbesteding) draaien. De schade is mogelijk ernstig als het lukt om fysiek toegang te krijgen tot de apparatuur van deze gemeentelijk informatiesystemen en/of gegevens. Afhankelijk van de implementatie (bijvoorbeeld netwerkscheidingen en virtualisatie) bestaat de mogelijkheid dat dit via omgevingen van derde gebeurt.
- Incident: Via programmatuur met betrekking tot gegevens.
 - Foutieve of gemanipuleerde programmatuur.
 - Doorwerking van virussen/malware.
 - Afbreken van verwerking.

Bijvoorbeeld: Bij SaaS oplossingen staan de gegevens op apparatuur van derden, dit geldt ook als de gemeentelijke informatiesystemen op de infrastructuur van derden (uitbesteding) draaien. De schade is mogelijk ernstig als het lukt om via het netwerk/internet toegang te verschaffen tot deze gemeentelijk informatiesystemen en/of gegevens. Afhankelijk van de implementatie (bijvoorbeeld netwerkscheidingen en virtualisatie) bestaat de mogelijkheid dat dit via omgevingen van derde gebeurt. Mogelijke oorzaken zijn: verouderde browsers (met bekende kwetsbaarheden), virussen op de servers kunnen de verwerking verstoren.
- Incident: Via personen met betrekking tot gegevens.
 - (On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data.
 - Onbevoegde toegang door onbevoegden.
 - Onbevoegd kopiëren van gegevens.
 - Meekijken over de schouder door onbevoegden.
 - Onzorgvuldige vernietiging.
 - Niet toepassen clear screen/clear desk.
 - Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties).
 - Oneigenlijk gebruik van autorisaties.
 - Toegang verschaffen tot d.m.v. identiteitsfraude of social engineering.

Bijvoorbeeld: De kans is aanwezig dat door (on)opzettelijk handelen gegevens worden gelekt door in publieke ruimten onbedoeld een casus te bespreken (omgevingsbewustzijn). Voorkomen is moeilijk en eigenlijk niet mogelijk.

4.2 Meest relevante maatregeldoelstellingen

In deze paragraaf wordt een overzicht gegeven van de meest relevante maatregeldoelstellingen die uit de uitgevoerde diepgaande risicoanalyse naar voren zijn gekomen. Hier dient expliciete aandacht aan te worden besteed. Deze meest relevante maatregeldoelstellingen zijn:

- Het voorkomen dat beheeractiviteiten niet, niet goed of niet tijdig worden uitgevoerd. Dit dient voorkomen te worden door het duidelijk beschrijven, toewijzen en vastleggen van de verantwoordelijkheden, bevoegdheden, taken en werkafspraken. Van zowel de interne en

externe ICT-dienstverlener(s) op het gebied van beheeractiviteiten. Ook is het noodzakelijk om gebruik te maken van patchmanagement, wijzigingsbeheer en ontwikkel- en testprocedures. Maak afspraken over het gewenste inzicht (rapportage/logging) in de wijze waarop door de leveranciers wordt omgegaan met het beheer van het informatiesysteem en in het bijzonder de omgang met gegevens.

- Als de programmatuur wordt ontwikkeld door een leverancier en als SaaS dienst afgenomen door de gemeente, wordt de software door een hoster via de software leverancier gehost en ontsloten via de gemeente.
 - Hoe is de verdeling?:
 - Technische voorzieningen Hoster door software leverancier,
 - Technisch applicatiebeheer door Leverancier,
 - Functioneel applicatiebeheer door de gemeente.
- Het voorkomen dat de continuïteit van kritische bedrijfsprocessen en de hierbij betrokken informatievoorziening wordt verstoord. Om de continuïteit niet te verstoren is het noodzakelijk om gebruik te maken van back-up en restore-procedures en het redundant uitvoeren van kritische componenten.
- Het voorkomen van ongeautoriseerde toegang tot het informatiesysteem en de gegevens daarin. Dit betreft zowel de fysieke toegang door gebruikers en beheerders tot de computerruimte als de toegang op infrastructureel en systeem niveau. Besteed expliciet aandacht aan toegang door externe partijen (leveranciers). Zorg ervoor dat goede afspraken met leveranciers worden gemaakt die aansluiten op de eisen vanuit het informatiesysteem. Zorg er ook voor dat een bewerkersovereenkomst wordt afgesloten waar ook aandacht is voor de aanbevelingen van deze risicoanalyse.
 - De apparatuur van het centrale systeem is van een hosting provider (SaaS dienst software leverancier) er wordt met desktops en tablets gewerkt.
 - De thuisomgeving is belangrijk omdat medewerkers vanuit thuis, maar ook vanuit de klant met het informatiesysteem kunnen werken. Zorg ervoor dat mobiele apparaten alleen verbinding kunnen maken met het informatiesysteem middels een beveiligde tunnel.
- Het voorkomen van onzorgvuldige (opzettelijk of onopzettelijk) omgang met de gegevens die in het informatiesysteem zijn opgeslagen, door gebruikers en beheerders. Dit dient zowel met technische middelen afgedwongen te worden als door middel van opleiding en communicatie (awareness) worden voorkomen.
 - Zorg ervoor dat bij de leveranciers duidelijk is wat de classificatie is van de gegevens is waarmee wordt gewerkt en de eisen die aan de beschikbaarheid en integriteit worden gesteld. Het gaat hierbij om persoonsgegevens en gerelateerde zaak gegevens. Er komen ook gegevens uit de GBA, SUWI en CORV.
 - Zorg ervoor dat de hoster de gegevens binnen Europees grondgebied op hardware heeft staan.
 - Zorg ervoor dat alle medewerkers zich bewust zijn van de noodzaak van informatiebeveiliging in het algemeen en hoe om te gaan met het informatiesysteem in het bijzonder.

4.3 Vervolgstappen

Op basis van de diepgaande risicoanalyse worden de hierna beschreven vervolgstappen geadviseerd. Het is de verantwoordelijkheid van de proces-/systeemeigenaar met betrekking tot de informatievoorziening sociaal domein om (in overleg met de informatiebeveiliging

coördinator of de Chief Information Security Officer (CISO) zorg te dragen voor de afhandeling van deze aanbevelingen.

1. Detaillering maatregelen.

Detailleer de in dit document (zie bijlage 1 maatregeldoelstellingen informatievoorziening sociaal domein) beschreven maatregeldoelstellingen naar concrete maatregelen, zodanig dat invulling wordt gegeven aan de beoogde doelstellingen. Hiervoor is de systeemeigenaar verantwoordelijk⁶ en kunnen de informatiebeveiliging coördinatoren of CISO ondersteuning leveren. Maak gebruik van de voorbeeldmaatregelen die zijn benoemd.

2. Acceptatie risico.

Als de maatregelen zijn bepaald, is het noodzakelijk dat het management vaststelt of de maatregel wel of niet wordt geïmplementeerd en/of in een andere vorm wordt geïmplementeerd. Bij de keuze om een maatregel niet of in een andere vorm te implementeren, hoort een expliciete risicoafweging die dient te worden vastgelegd.

3. Implementatie maatregelen.

Overleg per detailmaatregel met de informatiebeveiliging coördinator of de CISO van de gemeente over de implementatiewijze. Bepaalde maatregelen zijn specifiek voor het informatiesysteem terwijl andere maatregelen gemeentebreed opgepakt dienen te worden. De maatregelen die geïmplementeerd worden, dienen in een informatiebeveiligingsplan te worden beschreven (wie doet wat en wanneer en kosten). Beschrijf daarna per detailmaatregel wat de invulling en vindplaats is, aan de hand waarvan de implementatie (bestaan en werking) kan worden vastgesteld

4. Borging/control maatregelen.

Zorg voor een proces waarmee de borging van de maatregelen wordt gegarandeerd. In dit proces is het noodzakelijk dat periodiek op de aanwezigheid (het “bestaan”) en de juiste werking (de “werking”) van de maatregelen worden getoetst.

⁶ Als de verantwoordelijke nog niet bekend is dient deze te worden vastgesteld.

Bijlage 1: maatregeldoelstellingen informatievoorziening sociaal domein

Legenda:

OPM = opmerking

VBM = Voorbeeldmaatregel

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	Implementatiewijze (in te vullen door organisatie)
IB-beleid en plan	<p>Zorg voor aansluiting bij gemeentelijk beleid met betrekking tot wachtwoorden en systeem autorisaties.</p> <p>Zorg dat een bewerkersovereenkomst wordt afgesloten met nadruk op de volgende punten:</p> <ul style="list-style-type: none"> • Toegang tot apparatuur en software • Gedrag medewerkers bewerker door middel van bewustwording en geheimhoudingsverklaringen • Veilig vernietigen van gegevens en maken van back-ups en omgang met back-up media <p>Zorg dat afspraken met leveranciers worden gemaakt die aansluiten op de eisen vanuit het informatiesysteem.</p>	<p>OPM: controleer het gemeentelijk beveiligingsbeleid op deze punten, pas zo nodig aan bij de volgende herziening. Maak gebruik van het BIG-OP product Voorbeeld informatiebeveiligingsbeleid gemeenten.⁷</p> <p>OPM: Maak gebruik voor het opstellen van de bewerkersovereenkomst van het BIG-OP product Bewerkersovereenkomst.⁸</p> <p>OPM: Maak gebruik voor het vaststellen van de eisen van de baselinetoets BIG en eventueel de diepgaande risicoanalyse.</p> <p>OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier gebruik van de BIG-OP producten Contractmanagement.⁹ Inkoopvoorwaarden en informatiebeveiligingseisen.¹⁰ Service level agreements (in ontwikkeling).</p>	
Organisatie IB	Zorg voor een proces van continue aandacht voor informatiebeveiliging ten aanzien van het informatiesysteem. Verantwoordelijkheid ligt bij de systeemeigenaar.	VBM: Richt een cyclus in waarbij de beveiliging van regelmatig wordt geëvalueerd en bijgesteld. Daarbij hoort ook het opnieuw iken van de risicoanalyse bij relevante wijzigingen.	Zit reeds in de BIG, moet nog wel worden ingericht.
Classificatie en beheer van	Zorg ervoor dat alle medewerkers zich bewust zijn van	OPM: Maak gebruik voor het samenstellen van het	Zit reeds in de BIG als algemene maatregel. De

⁷ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-0919-voorbeeld-informatiebeveiligingsbeleid-gemeenten-1.0.pdf>

⁸ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0218-bewerkersovereenkomst-v1.0.pdf>

⁹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

¹⁰ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

informatie en bedrijfsmiddelen	<p>de noodzaak van informatiebeveiliging in het algemeen en hoe om te gaan met het informatiesysteem in het bijzonder.</p> <p>Zorg ervoor dat bij de leveranciers duidelijk is wat de classificatie is van de gegevens waarmee wordt gewerkt en de eisen die aan de beschikbaarheid en integriteit worden gesteld. Denk aan vastlegging in contracten richting de ICT leverancier</p>	<p>bewustwordingsprogramma van het BIG-OP personeelsbeleid (in ontwikkeling) en communicatieplan (in ontwikkeling). Bewustwordingscursussen Bespreken onderwerp informatieveiligheid bij beoordelingen</p> <p>OPM: Maak gebruik voor het vaststellen van de classificatie van de gegevens van het BIG-OP product Handreiking dataclassificatie.¹¹ OPM: Maak gebruik voor het vaststellen van de eisen van de Baselinetoets v1.0¹² en eventueel de diepgaande risicoanalyse.¹³ OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier gebruik van de BIG-OP producten Contractmanagement¹⁴, Inkoopvoorwaarden en informatiebeveiligingseisen¹⁵. Service level agreements (in ontwikkeling).</p> <p>OPM: Aandacht voor beveiligingseisen in het Programma van Eisen Specifieke eisen opnemen in contract, SLA en bewerkersovereenkomst met de leverancier.</p> <p>Bewaak de naleving</p>	<p>gemeente moet wel aandacht hebben voor specifieke eisen in contracten, SLA en bewerkersovereenkomst met Leverancier, waarbij ook aandacht is voor de hosting partij.</p> <p>De naleving moet jaarlijks worden getoetst.</p>
Personele beveiligingseisen	<p>Zorg ervoor dat de medewerkers en functioneel beheerders voldoende beschikbaar en getraind zijn om de werkzaamheden betrouwbaar uit te voeren. Er moet in bewustwording aandacht zijn voor de gevoeligheid van het werk en de gegevens en de risico's</p>	<p>OPM: Maak gebruik voor het samenstellen van het bewustwordingsprogramma van het BIG-OP personeelsbeleid (in ontwikkeling) en communicatieplan (in ontwikkeling) en Telewerkbeleid gemeente.¹⁶</p>	<p>bewustwordingspresentatie van de BIG-OP kan gebruikt worden met aanscherping op de punten welke links genoemd zijn.</p>

¹¹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1018-handreiking-dataclassificatie.pdf>

¹² <http://www.ibdgemeenten.nl/wp-content/uploads/2014/06/14-0609-BIG-Baselinetoets-v1.0.pdf>

¹³ <https://www.ibdgemeenten.nl/wp-content/uploads/2014/08/14-0806-Diepgaande-risicoanalyse-methode-gemeenten-v1.0-2.pdf>

¹⁴ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

¹⁵ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

¹⁶ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0410-Telewerkbeleid-gemeente-v1.0.pdf>

	<p>van onjuiste software op de thuiswerkplek. Er moet aandacht zijn voor het niet delen van wachtwoorden en autorisaties. In bewustwording aandacht voor omgaan met gegevens, zoals:</p> <ul style="list-style-type: none"> • Clear desk/ clear screen • Praten in openbaar • Vernietigen van notities/ informatie op papier • Shouldersurfing • Delen/gebruik van autorisaties <p>Jaarlijks herhalen en registratie van bezoek Logging gebruikers acties</p> <p>Maak afspraken met de leveranciers over eisen die aan medewerkers worden gesteld m.b.t. de omgang met gegevens in het informatiesysteem. Denk aan awareness en waar nodig/mogelijk geheimhoudingsverklaring.</p>	<p>OPM: Geef bewustwordingscursussen met aandacht voor gevoeligheid van het werk, de informatie, de risico's van onjuiste software. Heb aandacht voor het feit dat er logging plaatsvindt en dat gebruikers hun account gegevens niet mogen delen. OPM: Ook in deze bewustwording cursus aandacht voor omgaan met gegevens, zoals:</p> <ul style="list-style-type: none"> • Clear desk/ clear screen • Praten in openbaar • Vernietigen van notities/ informatie op papier • Shouldersurfing • Delen/gebruik van autorisaties <p>Er moet worden bijgehouden wie deze cursus gedaan heeft en er dient bij wijzigingen en periodiek herhaling van de cursus plaats te vinden. OPM: Specifieke systeem opleidingen OPM: Goede systeemdokumentatie OPM: Goede en actuele handleidingen</p> <p>OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier gebruik van de BIG-OP producten Contractmanagement¹⁷, Inkoopvoorwaarden en informatiebeveiligingseisen¹⁸, Service level agreements (in ontwikkeling).</p>	<p>Er moet worden bijgehouden wie deze cursus gedaan heeft en er dient bij wijzigingen en periodiek herhaling van de cursus plaats te vinden.</p> <p>De systeem gerelateerde documentatie voor eindgebruikers en functioneel beheerders dient te worden onderhouden en beschikbaar gesteld aan de gebruikers van het systeem.</p>
Fysieke beveiliging	<p>Zorg ervoor dat er ook inzicht komt op bezoekers aan de fysieke locatie van de ICT bij de hosting partij</p>	<p>OPM: Maak gebruik voor het verkrijgen van inzicht in de toegang tot fysieke locaties gebruik van het BIG-OP product Toegangsbeleid.¹⁹</p> <p>OPM: Om zicht te krijgen wie de fysieke systemen bezocht heeft (voor bijvoorbeeld</p>	<p>Zorg ervoor dat dit geregeld is in contracten met de leverancier. Binnen het informatiesysteem staan veel gegevens welke niet in verkeerde handen mogen vallen.</p>

¹⁷ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

¹⁸ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

¹⁹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/Toegangsbeleid.pdf>

	<p>Maak goede afspraken over de fysieke beveiliging van werkplekken binnen de gemeente en de leverancier waar bulk gegevens vanuit het informatiesysteem zijn opgeslagen. (denk aan Leverancier, de hoster en de gemeente)</p>	<p>beheerwerkzaamheden) dient een bezoekersregistratie te worden bijgehouden, dit punt is ook van toepassing op de SaaS leverancier en de hoster.</p> <p>OPM: De werkplek waarop bulk gegevens staan moet voldoende zijn beveiligd tegen ontvreemding van deze gegevens</p> <p>OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier gebruik van de BIG-OP producten Contractmanagement²⁰, Inkoopvoorwaarden en informatiebeveiligingseisen²¹, Service level agreements (in ontwikkeling).</p>	
Beheer van communicatie- en bedieningsprocessen	<p>Zorg voor een opleiding van alle gebruikers en beheerders voor het beheren en gebruiken van het systeem</p> <p>Zorg ervoor dat mobiele apparaten alleen verbinding kunnen maken met het informatiesysteem middels een beveiligde tunnel.</p>	<p>OPM: Maak gebruik voor het samenstellen van het bewustwordingsprogramma van het BIG-OP personeelsbeleid (in ontwikkeling) en communicatieplan (in ontwikkeling). Voor beheerders geldt mogelijk een andere bewustwording cursus dan voor eindgebruikers, dit omdat bij beheerders door de omvang van de gegevens de risico's van inzage en fouten toenemen.</p> <p>OPM: Maak gebruik voor het beheer van mobiele apparaten en netwerkverbindingen van de BIG-OP producten Mobile Device Management²² en Telewerkbeleid gemeente²³.</p> <p>OPM: Bij mobiele toegang van buiten de gemeente dient altijd gebruik te worden gemaakt van een</p>	Zorg ervoor dat dit geregeld is in contracten met de leverancier.

²⁰ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

²¹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

²² <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1007-Mobile-Device-Management.pdf>

²³ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0410-Telewerkbeleid-gemeente-v1.0.pdf>

	<p>Zorg voor duidelijke procedures voor de applicatiebeheerder met aandacht voor gegevensbeheer en autorisatiecontrole</p> <p>Maak afspraken over het gewenste inzicht (rapportage/logging) in de wijze waarop door de leveranciers wordt omgegaan met het beheer van het informatiesysteem en in het bijzonder de omgang met gegevens.</p>	<p>beveiligde tunnel.</p> <p>OPM: Maak gebruik voor gegevensbeheer (classificatie) gebruik van de BIG-OP producten Handreiking dataclassificatie²⁴ en logische toegangsbeveiliging.²⁵</p> <p>VBM: Alle elektronische toegang wordt gelogd.</p> <p>OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier (over logging/monitoring) gebruik van de BIG-OP producten Aanwijzing Logging²⁶ Contractmanagement²⁷, Inkoopvoorwaarden en informatiebeveiligingseisen²⁸. Service level agreements (in ontwikkeling).</p>	
Logische Toegangsbeveiliging	<p>Zorg ervoor dat als een tablet gebruikt gaat worden die buitenom de virtuele desktop gaat, dient er gebruik gemaakt te worden van een MDM oplossing.</p> <p>Zorg voor het beperken van toegang tot de webpagina's, eventueel beperkte functionaliteit binnen de webserver voor mobiele apparaten.</p> <p>Zorg ervoor dat de gemeente het MDM beheer uitvoert of laat uitvoeren en monitort voor alle mobiele apparaten die het informatiesysteem kunnen en mogen benaderen.</p>	<p>OPM: Maak gebruik voor het beheer van mobiele apparaten en netwerkverbindingen van de BIG-OP producten Mobile Device Management²⁹ en Telewerkbeleid gemeente.³⁰</p> <p>OPM: Met name de wijze waarop remote toegang wordt gecontroleerd is van belang.</p> <p>OPM: de MDM oplossing dient ertoe om mobiele apparaten op afstand te beheren, lokale opslag te beperken en te beschermen. Remote wipen moet tot</p>	

²⁴ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1018-handreiking-dataclassificatie.pdf>

²⁵ <https://www.ibdgemeenten.nl/wp-content/uploads/2014/08/14-0731-Beleid-logische-toegangsbeveiliging-v1.0-1.pdf>

²⁶ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

²⁷ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

²⁸ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

²⁹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1007-Mobile-Device-Management.pdf>

³⁰ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0410-Telewerkbeleid-gemeente-v1.0.pdf>

	<p>Zorg ervoor dat indien een tablet gebruikt wordt dat er geen gegevens op het tablet of mobile apparaat terecht kunnen komen of opgeslagen worden.</p> <p>Heb aandacht voor logging op de webserver met name voor mobile devices</p> <p>Zorg ervoor dat de applicatie aangeboden dient te worden door middel van een vorm van virtualisatie waar alleen beeldscherm inhoud wordt getransporteerd om de kans te verkleinen dat informatie gelekt wordt vanaf het te gebruiken apparaat (desktop, tablet). Waarbij minimaal 2 factor Authenticatie wordt toegepast</p> <p>Zorg ervoor dat binnen het systeem er expliciet rechten moeten worden gegeven op een zaak, logging, rapportage en controle door de procesondersteuner rapportage naar manager. Zorg ervoor dat alleen geautoriseerde personen toegang hebben tot de gegevens in het informatiesysteem en in het bijzonder tot de vertrouwelijke gegevens.</p> <p>Zorg ervoor dat gegevens die in het gemeentelijke zaaksysteem en DMS worden opgeslagen de zelfde toegangsregels te hebben als de gegevens in de zorgapplicatie, met name als er meer dan alleen "dat" informatie wordt opgeslagen.</p> <p>Zorg ervoor dat alle toegang tot informatie wordt gelogd, in welk gemeentelijk systeem ook gerelateerd aan het proces en systeem.</p> <p>Bij voorkeur wordt alleen DAT informatie opgeslagen en niet WAT informatie, gebruik maken van StUF zaken bericht met procesinformatie</p> <p>Zorg ervoor dat dossiers en informatie die in het DMS terecht komt als vertrouwelijk kan worden aangemerkt</p>	<p>te mogelijkheden behoren.</p> <p>OPM: streef na dat alle toegang op afstand op eenzelfde manier wordt beveiligd, bijvoorbeeld de remote desktop middels Citrix, dan ook de remote tablet middels Citrix, dit voorkomt beheerfouten en het gebruik van deze virtualisatie zorgt ervoor dat aan MDM minder strenge eisen hoeven te worden gesteld,</p> <p>OPM: Maak gebruik voor gegevensbeheer (classificatie) gebruik van de BIG-OP producten Handreiking dataclassificatie³¹ en logische toegangsbeveiliging.³²</p> <p>VBM: in aanvulling op hoofdstuk 11.6 van de tactische baseline:</p> <p>De toegang tot gevoelige informatie wordt toebedeeld door de casemanager/procesondersteuner op need to know basis. Alle toegangswijzigingen worden gelogd. Periodiek wordt over rechten gerapporteerd aan de manager.</p> <p>OPM: het risico bestaat dat in het DMS informatie terecht komt waar de beheerders van het DMS geen inzage recht op hebben. (bijvoorbeeld medisch geheim) Voorkom dat gevoelige informatie in het DMS systeem terechtkomt door het opstellen van regels wat wel en niet in het DMS opgeslagen mag worden. Zitten hier toch gevoelige gegevens bij dient de toegang tot die gegevens te worden gelogd.</p>	
--	---	---	--

³¹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1018-handreiking-dataclassificatie.pdf>

³² <https://www.ibdgemeenten.nl/wp-content/uploads/2014/08/14-0731-Beleid-logische-toegangsbeveiliging-v1.0-1.pdf>

	<p>en dat niet zomaar door iedereen dit kan worden gelezen lezen</p> <p>Maak afspraken over de (remote) toegang tot het informatiesysteem door beheerders, ontwikkelaars et cetera.</p> <p>Zorg voor een voldoende en recente antivirussoftware om virussen tegen te gaan zowel voor de desktop, en de servers</p> <p>Zorg voor het ontwikkelen van en naleven van indienst, uitdienst en functie verandering procedures, logging, rapportage en periodieke controle (kwartaal) door de manager</p>	<p>OPM: Maak gebruik voor de antivirussoftware gebruik van Anti malware beleid³³</p> <p>OPM: Maak gebruik voor het samenstellen van deze procedures van het BIG-OP product personeelsbeleid (in ontwikkeling).</p> <p>OPM: zie voor personele beveiligingsmaatregelen hoofdstuk 8 van de tactische BIG</p>	
Ontwikkeling en onderhoud van systemen	<p>Zorg ervoor dat er goede systeem documentatie worden gemaakt en onderhouden.</p> <p>Zorg ervoor dat door de ontwikkelaar gebruik gemaakt wordt van gescheiden omgevingen (OTAP) en duidelijke procedures.</p> <p>Zorg ervoor dat de invulling en instandhouding van beveiligingsmaatregelen onderdeel zijn van de afspraken m.b.t. ontwikkeling en onderhoud.</p>	<p>OPM: Maak gebruik van het BIG-OP product Handreiking proces wijzigingsbeheer³⁴</p>	
Beheer van beveiligingsincidenten	<p>Zorg ervoor dat vanuit de leverancier tijdig informatiebeveiligingsincidenten worden gemeld</p>	<p>OPM: Maak gebruik van het BIG-OP product Voorbeeld incident management en response beleid³⁵</p>	
Continuïteit	<p>Zorg voor een visie/aanpak hoe om te gaan met de eis die wordt gesteld aan de continuïteit van het</p>	<p>OPM: Moet wellicht onderdeel zijn van een gemeente brede aanpak voor het organiseren van</p>	

³³ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1008-Anti-malware-beleid-1.0.pdf>

³⁴ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0410-Handreiking-proces-wijzigingsbeheer-v1.0.pdf>

³⁵ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1111-voorbeeld-incident-management-en-response-beleid.pdf>

	<p>informatiesysteem</p> <p>Vertaal de visie/aanpak voor continuïteit van het informatiesysteem naar eisen die aan de leveranciers worden gesteld.</p>	<p>de gewenste continuïteit. Heb hierbij ook aandacht voor het feit dat systemen bij de hoster soms gegevens nodig hebben van gemeentelijke systemen en omgekeerd.</p> <p>OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier (over logging/monitoring) gebruik van de BIG-OP producten Aanwijzing Logging³⁶, Contractmanagement³⁷, Inkoopvoorwaarden en informatiebeveiligingseisen³⁸, Service level agreements (in ontwikkeling).</p>	
Naleving	<p>Zorg ervoor dat de controle van extern betrokken diensten onderdeel is van het reguliere demand proces.</p> <p>Zorg voor controle van de diensten die door leveranciers worden geleverd om de aanwezigheid en juiste werking van beveiligingsmaatregelen garanderen.</p>	<p>OPM: Maak gebruik voor het vastleggen van de afspraken met de leverancier (over logging/monitoring) gebruik van de BIG-OP producten Aanwijzing Logging³⁹, Contractmanagement⁴⁰, Inkoopvoorwaarden en informatiebeveiligingseisen⁴¹, Service level agreements (in ontwikkeling).</p> <p>OPM: Heb aandacht voor beveiligingseisen in de contracten, de SLA en de bewerkersovereenkomst en controleer de naleving</p>	

³⁶ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

³⁷ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

³⁸ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

³⁹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

⁴⁰ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0408-Contractmanagement-v1.0.pdf>

⁴¹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0212-Inkoopvoorwaarden-en-informatiebeveiligingseisen-v1.0.pdf>

